How Safe is Safe Enough?

1. Chapter 1 of *Safeware* argues for a shift of responsibility for controlling risk from individuals and personal responsibility to organizational or public responsibility. On the other hand, public accountability tends to lessen as professional roles become narrowly differentiated.

   Consider the following reasonable and common views of various professional roles today:

   - **Operators and workers**: I am given training and procedures to follow. If those are wrong, I cannot be held responsible. In addition, I am limited by the information the automation gives me about the state of the system. I cannot be held responsible for flawed design of the system with which I have to interact, which is often very difficult or clumsy to operate.
   - **System Engineer**: My responsibility is to receive directives and to create products given the requirements and sometimes specifications set by others. The decision about what products to make and their general specifications are economic in nature and made by management. When parts of the system are subcontracted to others or commercial off-the-shelf components are used, the internal design of these components is often claimed to be proprietary, and I am not allowed to inspect or review them. Therefore I cannot be held responsible for the content or effects.
   - **Hardware Engineer**: My responsibility is to receive directives and to create components given the requirements and sometimes specifications set by others. I have no control over how my hardware and software components are used. Therefore I cannot be held responsible if they are used in a dangerous way.
   - **Software engineer**: I am provided with a set of requirements that I implement. I do not have the training in engineering to make judgements about whether they are reasonable or not. My job is simply to code what I am asked to code.
   - **Researcher**: My responsibility is to gain knowledge. How the knowledge is applied is an economic decision made by management or else a political decision made by elected representatives in government.
   - **Manager**: My responsibility is solely to make profits for stockholders.
   - **Stockholder**: I invest my money for the purpose of making a profit. It is up to managers to make decisions about the directions of technological development.
   - **Consumer**: My responsibility is to my family. Government should make sure corporations do not harm me with dangerous products, harmful side effects of technology, or dishonest claims. I usually do not have the information nor competence to make such evaluations myself.
   - **Government regulator**: By current reckoning, government has strangled the economy through over-regulation of business. Accordingly at present on my job, especially given decreasing budget allocations, I must back off from the idea that business should be policed. Instead I will urge corporations to assume greater public responsibility. In addition, I cannot look through millions of lines of software code and sometimes thousands of physical components in a product to determine whether it is safe. I need to put trust in the engineers who create these systems.

   Also, consider the following accident:

[From Schinzinger, page 102] On February 26, 1972, the Buffalo Creek dam near Lorado, West Virginia, collapsed, "unleashing a wall of water that killed 118 persons and swept away four communities." A U.S. Senate labor subcommittee investigating the damage found that "lack of adequate design and construction measures as well as the poor planning and operation make all similar dams presently in use a serious hazard ... The safety factor slipped between the cracks of responsibility." Regulations of the U.S. Bureau of Mines called for inspections that had not been carried out. But, stated the Bureau's director, "Even if a bureau coal mine inspector had been at the dam site as the water rose, his authority would have been limited to the issuance of an imminent danger order, withdrawing the mine workers on the mine property." It would not, he said, have "prevented the retaining dam from falling nor would it have been applicable to persons off the mine property in the path of the flood."

The West Virginia Public Service Commission denied responsibility because it certifies dams for safety only at the time that a builder applies for a permit to build a dam. The Commission claims to have no jurisdiction over dams once they have been built (based on an Associated press report in the Los Angeles Times, 1 June 1972).

A Governor's Ad Hoc Committee found that the dam had been built by a non-engineer, that inspectors should have been aware of problems, and that the engineering profession should have sounded a warning since some of its members were aware of the substandard construction. The registration system had failed in this instance, because "the speciality required by any engineer designing and constructing such a one as that which failed, is not covered in any of the categories mentioned by the West Virginia State Registration Board. Moreover, since the technology of building such dams as this had not been developed, there was no way of judging any competence in the persons constructing the dams (in The West Virginia Engineer, December 1972, courtesy of Robert D. Miles, Purdue University).

New technology must also be considered. Dependence on computers has intensified the division of labor within engineering. For example, civil engineers designing a flood control system have to rely on information and programs obtained from systems analysts and implemented by computer programmers. The systems analysts could argue they have no moral or legal responsibility for the safety of the people affected by the flood control plans because are merely providing tools whose use is entirely up to the engineers. Should the civil engineers be held accountable for any harm caused by poor computer programs? Presumably their accountability does extend to errors resulting from their own inadequate specifications that they supply to the computer experts. Should engineers be expected to contract with computer specialists who agree to be partially accountable for the end-use effects of their program?

As an example, in 1979 an error was discovered in a program used to design nuclear reactors and their supporting cooling systems [101]. The erroneous part of the program dealt with the strength and structural support of pipes and valves in the cooling system. The program had supposedly guaranteed the attainment of earthquake safety precautions in operating reactors. The discovery of the program error resulted in the Nuclear Regulatory Commission shutting down five nuclear power plants.

Written and in-class discussion question: Who do you think should be responsible for risk management today, i.e., government regulatory agencies, individuals, industrial manage-

ment, workers, engineers, researchers, safety experts, public lobbies and consumer groups, insurance companies and voluntary evaluation groups like UL, or the court system? What role in risk management do you think each of these groups should play today? What affect does new and rapidly changing technology have on these issues?

2. Consider the following two quotes:

From *Science*, July 10, 1981:

> The Supreme Count in the cotton dust decision on 17 June, says explicitly that OSHA must ignore the results of any cost-benefit comparison when setting a standard for worker exposure to a hazardous substance. Justice William Brennan, writing for the court's five-person majority, said that "Congress itself decided the basic relationship between costs and benefits by placing the benefit of the worker's health above all other considerations when it wrote the law in 1970. Yet the agency cannot require exposure controls that are impossible to achieve, nor can it bankrupt an entire industry," He concluded consideration of anything besides these questions would be inconsistent with Congress's direction.

And from T.W. Lockhart, "Safety Engineering and the Value of Life," Technology and Society (IEEE), vol. 9, March 1981, pp. 3-5:

> ...there is an honored tradition in moral philosophy, associated primarily with Immanuel Kant, according to which human beings have a worth that is not commensurate with that of mere objects. According to this view, because of this incommensurability we must recognize and respect the liberty and dignity of each person and refrain from treating him merely as a means to some end. Human beings may not be used in order to achieve some higher good, for there is no higher good. Let us call this view the *Incommensurability Principle.*
>
> The Incommensurability Principle has had a powerful appeal for many. This has been true mainly because it has been felt that unless it, or something like it, is accepted it is not possible to account for such fundamental human rights as the right not to be killed, the right not to have one's liberty abridged without just cause, and the right to be treated fairly and honestly. The Incommensurability Principle is clearly incompatible with an attempt to place a monetary value on human life or to justify actions on the basis of such a valuation. There is thus further reason for doubting the wisdom of any such attempt ...

Is it possible to reconcile the Incommensurability Principle with the view that considerations of safety must be weighed against economic costs (the use of cost/risk–benefit analysis)? The Ford Pinto case is an example of the principle involved here. How does this relate to the Cotgrove ideas presented at the end of Chapter 1 in *Safeware* about differing value systems?

Read the Sundstein article for a recent example of this debate. Write (no more than a page or so) your own preliminary views on these questions above.

3. What role should the courts and legal system play? Consider the following two cases:

   - Employers who expose their employees to safety hazards usually escape criminal penalties. Victims will often sue companies for damages under tort (i.e., civil) law, which allows them to gain compensation without having to prove a crime has been committed. This is true even when people die as a result of horrendous corporate negligence.

     No example is more shocking than that of the companies in the asbestos industry, especially Manville Corporation (formerly Johns-Manville Corp.), which is the largest producer of asbestos. Manville knew from the 1930s and 1940s onward that asbestos fibers in the lungs cause asbestosis, an incurable form of cancer. For three decades it concealed this information from workers and the public who had a right to give informed consent to the dangers confronting them. In 1949, Manville's company physician defended a policy of not informing employees diagnosed with asbestosis: "As long as the man feels well, is happy at home and at work and his physical condition remains good, nothing should be said." (Brodeur, 1985). When Manville was finally brought to trial, company officials claimed that some 1300 of the company's own studies of asbestos had mysteriously disappeared from its files.

     One recent study showed that 38 percent of asbestos insulation workers die of cancer, 11 percent from asbestosis. It is predicted that "among the twenty-one million living American men and women who had been occupationally exposed to asbestos between 1940 and 1980, there would be between eight and ten thousand deaths from asbestos-related cancer each year for the next twenty years." The actor Steve McQueen is just one individual included among these grim statistics. In his youth, he held a summer job handling asbestos insulation and two decades later died of asbestosis.

     In order to postpone settling the flood of lawsuits, Manville filed for bankruptsy in 1982. (Its assets of $2 billion made it the largest American corporation ever to do so). A court agreement reached in 1985 allows it to continue operating while paying some $2.5 billion in lawsuits over the next 25 years.

   - In 1985, for the first time in history, a judge convicted three officials of a company for industrial murder (Frank, 1987). Film Recovery Systems was a small corporation which recycled silver from used photographic and x-ray plates. Used plates were soaked in a cyanide solution to leach out their silver content. Other companies use this process safely by protecting workers against inhaling cyanide gas and making skin contact with the liquid. Standard safety equipment includes rubber gloves, boots, and aprons, as well as respirators and proper ventilation. None of these precautions were used by Film Recovery Systems. Workers were given useless paper face masks and cloth gloves. Ventilation was terrible, and respirators were not provided. Workers frequently became nauseated and had to go outside to vomit before returning to work at the cyanide vats. This continued until an autopsy on one employee, a Polish immigrant, revealed lethal cyanide poisoning. Charges were brought against the executives of Film Recovery Systems under an Illinois statute which states that "a person who kills an individual without lawful justification commits murder if, in performing the acts which cause the death ... he knows that such acts create a strong probability of death or great bodily harm to that individual or another." (Frank, 1987). During the trial, it was proven that the company president, the plant manager, and the plant foreperson all knew of the dangers of cyanide. They also knew about the hazardous conditions at their plant. Each was sentenced to 25 years in jail and fined $10,000. Critics have disagreed with

this conviction on the grounds that murder involves intentional and purposeful killing. At most, say the critics, the executives committed manslaughter, which is killing due to negligence or indifference (such as when drunk drivers kill). Do you think the executives of Film Recovery Systems should be charged with manslaughter, murder, or no crime at all?

Another example is the Concorde trial going on right now.

Written question: What role should the courts and lawyers play in ensuring public safety?

16.863J / ESD.863J System Safety
Spring 2011